Suricata with Wazuh

*Installation de Suricata

Infrastructure

Endpoint	Description
ubuntu 24	This is the endpoint where you install Suricata. In this use case, Wazuh monitors and analyzes the network traffic generated on this endpoint.

Installation

from UBUNTU

```
sudo add-apt-repository ppa:oisf/suricata-stable

sudo apt-get update

sudo apt-get install suricata -y
```

Téléchargement des règles Suricata

```
cd /tmp/ && curl -LO https://rules.emergingthreats.net/open/suricata-6.0.8/emerging.rules.tar.gz

sudo tar -xvzf emerging.rules.tar.gz && sudo mkdir /etc/suricata/rules && sudo mv rules/*.rules /etc/suricata/rules/

sudo chmod 640 /etc/suricata/rules/*.rules
```

Modifier les paramètres de Suricata

```
/etc/suricata/suricata.yaml

HOME_NET: "<UBUNTU_IP>"
EXTERNAL_NET: "any"

default-rule-path: /etc/suricata/rules
rule-files:
- "*.rules"

# Global stats configuration
stats:
enabled: yes

# Linux high speed capture support
af-packet:
  - interface: enp0s3
```

// Changer "interface" par sa propre carte Ethernet //

Pour obtenir le nom de sa carte Ethernet :

ifconfig

```
Output

**enp0s3:** flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet @IP  netmask @NET  broadcast @IP

        ether 08:00:27:14:65:bd  txqueuelen 1000  (Ethernet)
        RX packets 6704315  bytes 1268472541 (1.1 GiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4590192  bytes 569730548 (543.3 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Redémarrer les services

```
sudo systemctl restart suricata
sudo systemctl status suricata
```

```
● suricata.service - Suricata IDS/IDP daemon
     Loaded: loaded (/lib/systemd/system/suricata.service; enabled; preset: ena>
     Active: active (running) since Mon 2025-04-07 16:08:24 CEST; 1min 3s ago
       Docs: man:suricata(8)
             man:suricatasc(8)
             https://suricata-ids.org/docs/
    Process: 3387 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/s>
   Main PID: 3389 (Suricata-Main)
      Tasks: 8 (limit: 2241)
     Memory: 50.2M
        CPU: 1.797s
     CGroup: /system.slice/suricata.service
             └─3389 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.>

avril 07 16:08:24 suricata systemd[1]: Starting suricata.service - Suricata IDS>
avril 07 16:08:24 suricata suricata[3387]: 7/4/2025 -- 16:08:24 - <Notice> - Th>
avril 07 16:08:24 suricata systemd[1]: Started suricata.service - Suricata IDS/>
lines 1-17/17 (END)
```

Intégration Wazuh

// Installation de l'agent Wazuh nécessaire au préalable //

Ajouter cette configuration à l'agent Wazuh :

On indique à l'agent de surveiller les logs de Suricata

```
<ossec_config>
  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>
</ossec_config>
```

```
sudo systemctl restart wazuh-agent
```

Attack emulation

Ping the Ubuntu endpoint IP address from the Wazuh server:

```
ping -c 20 "<UBUNTU_IP>"
```

Depuis le Dashboard Wazuh :

PING

>	Apr 25, 2025 @ 10:52:17.994	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:17.989	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:15.986	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:15.986	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:13.985	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:13.985	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:11.983	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:11.983	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:09.984	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:09.982	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:07.981	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:07.979	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:05.979	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:05.977	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:03.977	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:03.975	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata
>	Apr 25, 2025 @ 10:52:01.976	Suricata: Alert - GPL ICMP_INFO PING *NIX	86601	3	suricata

NMAP

	Time	rule.description	rule.id	rule.level	agent.name
>	Apr 25, 2025 @ 10:55:18.161	Suricata: Alert - ET SCAN Suspicious inbound to PostgreSQL port 5432	86601	3	suricata
>	Apr 25, 2025 @ 10:55:16.160	Suricata: Alert - ET SCAN Suspicious inbound to MSSQL port 1433	86601	3	suricata
>	Apr 25, 2025 @ 10:55:14.202	Suricata: Alert - ET SCAN Suspicious inbound to Oracle SQL port 1521	86601	3	suricata
>	Apr 25, 2025 @ 10:55:14.202	Suricata: Alert - ET SCAN Potential VNC Scan 5800-5820	86601	3	suricata
>	Apr 25, 2025 @ 10:55:14.158	Suricata: Alert - ET SCAN Suspicious inbound to mySQL port 3306	86601	3	suricata